Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (currently amended): A method for authenticating a sender of a digital object on a peer-to-peer (P2P) communication, comprising:

recognizing ~~a peer-to-peer (~~ the P2P~~)~~ communication between a first client and a second client, said first client attempting to exchange information securely with said second client via the P2P communication without a third party mediation, said third party mediation including certificate authorities;

in response to the recognized P2P communication, establishing an electronic mail protocol communication between the first client and the second client after the P2P communication is recognized, said e-mail protocol communication being a separate connection from the P2P communication, said e-mail protocol communication being established by Simple Mail Transport Protocol (SMTP);

generating a first unique identifier (UID);

transmitting from the first client to a previously known address of the second client, via the established electronic mail protocol communication, a first electronic mail (e-mail) message comprising the first UID;

receiving from the second client, via the electronic mail protocol communication, a second e-mail message directed to the first client, said second e-mail message comprising a second UID and a copy of the first UID;

verifying the copy of the first UID is identical to the first UID at the first client; and

transmitting from the first client to the previously known address of the second client, via the electronic mail protocol communication, a third e-mail message to the second client comprising a copy of the second UID;

wherein at least one of the e-mail messages transmitted to the previously known address between the first client and the second client further comprises the digital object, said digital object authenticating the information to be exchanged between the first client and the second

client via the P2P communication and not authenticating the first e-mail message, the second e-mail message, or the third e-mail message.

Claim 2 (original): The method of claim 1 wherein the first message further comprises the digital object.

Claim 3 (original): The method of claim 1 wherein the third message further comprises the digital object.

Claim 4 (original): The method of claim 1 wherein the digital object is a public key for a cryptographic system.

Claim 5 (previously presented): The method of claim 4 wherein the second message further comprises a second public key for the cryptographic system.

Claims 6-7 (canceled).

Claim 8 (original): The method of claim 1 wherein the first UID contains at least 128 bits.

Claim 9 (currently amended): A method for authenticating a sender of a digital object, comprising:

recognizing a peer-to-peer (P2P) communication between a first client and a second client, said first client attempting to exchange information securely with said second client via the P2P communication without a third party mediation, said third party mediation including certificate authorities;

in response to the recognized P2P communication, establishing an electronic mail protocol communication between the first client and the second client, said e-mail protocol communication being a separate connection from the P2P communication, said e-mail protocol communication being established by Simple Mail Transport Protocol (SMTP);

receiving from the first client, via the established electronic mail protocol communication, a first electronic mail (e-mail) message comprising a first unique identifier (UID);

generating a second UID at the second client;

transmitting from the second client to a previously known address of the first client, via the electronic mail protocol communication, a second e-mail message comprising the second UID and a copy of the first UID;

verifying the copy of the first UID is identical to the first UID at the first client; and

receiving at the second client, via the electronic mail protocol communication, a third e-mail message comprising a copy of the second UID from the first client after the first client has verified the copy of the first UID;

wherein at least one of the e-mail messages received further comprises the digital object, said digital object authenticating the information to be exchanged between the first client and the second client via the P2P communication and not authenticating the first e-mail message, the second e-mail message, or the third e-mail message.

Claim 10 (original): The method of claim 9 wherein the first message further comprises the digital object.

Claim 11 (original): The method of claim 9 wherein the third message further comprises the digital object.

Claim 12 (original): The method of claim 9 wherein the digital object is a public key for a cryptographic system.

Claim 13 (previously presented): The method of claim 12 wherein the second electronic mail message further comprises a second public key for the cryptographic system.

Claims 14-15 (canceled).

Claim 16 (original): The method of claim 9 wherein the first UID contains at least 128 bits.

Claim 17 (currently amended): A computer storage medium including computer-executable instructions facilitating authenticating a sender of a digital object on a peer-to-peer (P2P) communication, computer-executable instructions executing the steps of:

recognizing a peer-to-peer (P2P) communication between a first client and a second client, said first client attempting to exchange information securely with said second client via the P2P communication without a third party mediation, said third party mediation including certificate authorities;

in response to the recognized P2P communication, establishing an electronic mail protocol communication between the first client and the second client, said e-mail protocol communication being a separate connection from the P2P communication, said e-mail protocol communication being established by Simple Mail Transport Protocol (SMTP);

generating a first unique identifier (UID);

transmitting from the first client to a previously known address of the second client, via the established electronic mail protocol communication, a first electronic mail (e-mail) message comprising the first UID;

receiving from the second client, via the electronic mail protocol communication, a second e-mail message directed to the first client comprising a second UID and a copy of the first UID;

verifying the copy of the first UID is identical to the first UID at the first client; and

transmitting from the first client to the previously known address, via the electronic mail protocol communication, a third e-mail message to the second client comprising a copy of the second UID;

wherein at least one of the messages transmitted to the previously known address further comprises the digital object, said digital object including the information to be exchanged between the first client and the second client via the P2P communication and not authenticating the first e-mail message, the second e-mail message, or the third e-mail message.

Claim 18 (previously presented): The computer storage medium of claim 17 wherein the digital object is a public key for a cryptographic system.

Claim 19 (previously presented): The computer storage medium of claim 18 wherein the second message further comprises a second public key for the cryptographic system.

Claim 20 (currently amended): An apparatus for securely exchanging a public key without third party mediation, comprising:

a random number generator generating a first unique identifier (UID);

a network interface recognizing a peer-to-peer (P2P) communication between a first client and a second client, said first client attempting to exchange a public key securely with said second client via the P2P communication;

wherein, in response to the recognized P2P communication, the network interface establishes an electronic mail protocol communication between the first client and the second client, said e-mail protocol communication being a separate connection from the P2P communication, said e-mail protocol communication being established by Simple Mail Transport Protocol (SMTP);

wherein the network interface transmits to a previously known address associated with the second client, via the established electronic mail (e-mail) protocol communication, a first e-mail message comprising the first UID;

wherein the network interface receives, via the electronic mail protocol communication, a second e-mail message transmitted to a previously known address associated with the first client, said second e-mail message comprising a second UID and a copy of the first UID, wherein the copy of the first UID is compared to the first UID for verification thereof;

wherein the network interface transmits to the previously known address associated with the second client, via the electronic mail protocol communication, a third e-mail message comprising a copy of the second UID, wherein the copy of the second UID is compared to the second UID for verification thereof; and

wherein at least one of the e-mail messages transmitted to the previously known address associated with the second client further comprises the key by which the information to be exchanged between the first client and the second client via the P2P communication is secured and not authenticating the first e-mail message, the second e-mail message, or the third e-mail message.

Claim 21 (previously presented): The method of claim 1, further comprising, at the first client, using the e-mail address from the second client to index the first UID after verifying the copy of the first UID is identical to the first UID at the first client.

Claim 22 (previously presented): The method of claim 9, further comprising, at the second client, verifying the copy of the second UID is identical to the second UID at the second client and using the e-mail address from the first client to index the second UID after verifying.